UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF TENNESSEE

JENNIFER BANDY, on behalf of all others similarly situated, Plaintiff, v. TOC ENTERPRISES, INC., d/b/a Tennessee Orthopaedic Clinics, a division of TENNESSEE ORTHOPAEDIC ALLIANCE, P.A., Defendant.	Case No. 3:23-cv-00598 **SECOND AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

SECOND AMENDED CLASS ACTION COMPLAINT

Jennifer Bandy ("Plaintiff"), brings this Second Amended Class Action Complaint on behalf of herself, and all others similarly situated ("Class") against Defendant TOC Enterprises, Inc., d/b/a/ Tennessee Orthopaedic Clinics, a Division of Tennessee Orthopaedic Alliance, P.A. ("TOC" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities, and alleges as follows:

INTRODUCTION

1. On or about May 2, 2023, TOC, a comprehensive medical and surgical treatment center of bone, joint and soft tissue disorders, identified unusual activity on its networks. Upon investigating, TOC discovered that it had lost control of an undisclosed amount of former and current patients' highly sensitive personal records in a data breach by cybercriminals ("Data Breach").[1] Upon information and belief, the Data Breach occurred between March 20, 2023, and March 24, 2023.

[1] *See* https://www.tocdocs.com/notice-of-security-incident/ (last accessed July 20, 2023).

2. On or about May 19, 2023, TOC first notified the U.S. Department of Health and Human Services Office for Civil Rights ("HHS") of this breach on or about May 19, 2023, using a place-holder indicating that "500" individuals were affected. [2]

3. On or about July 13, 2023, almost two months later, TOC sent Data Breach Notice Letters ("Notice Letters") to victims of the Data Breach informing them that hackers had gained unauthorized access to their confidential personal identifying information ("PII") and/or personal health information ("PHI") (together "Private Information" or "PII"). *See* Collective Ex. A.

4. According to the Notice Letters, the stolen PII included, at least, names, contact information, dates of birth, diagnosis and treatment information, provider names, dates of service, cost of services, prescription information, and/or health insurance information.

5. Cybercriminals were able to breach TOC's systems because TOC did not maintain reasonable security safeguards or protocols to protect its patients' PII, leaving it an unguarded target for theft and misuse.

6. After the Data Breach ended on March 24, 2023, TOC did not notify the Data Breach victims about the breach within 45 days as required by Tennessee law, depriving them an opportunity to mitigate the Data Breach's impact on them and to secure their identities from theft.

7. When TOC finally publicly admitted to the Data Breach in May 2023 with an online breach notice ("Breach Notice"), it obfuscated the nature of the breach and the threat it posed—refusing to tell HHS or its patients how many people were affected, how the breach happened, or why it took over two months for TOC to send a bare-bones notice.[3] *See* Breach Notice Letter, attached as Exhibit A.

8. Despite the lifelong harm that the Data Breach poses to its current and former

[2] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed July 20, 2023).
[3] https://www.tocdocs.com/notice-of-security-incident/ (last accessed July 20, 2023).

patients, upon information and belief TOC has not offered the breach victims any credit or health privacy monitoring services.

9. TOC's failure to safeguard patients' Private Information and adequately warn them about the Data Breach violates Tennessee and federal law, harming thousands of individuals.

10. Plaintiff, as captioned above, is a current or former TOC patient who provided TOC with her Private Information, and upon information and belief, is a Data Breach victim, causing her to seek relief on a class-wide basis.

11. TOC knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

12. TOC's misconduct has injured the Plaintiff and members of the proposed Class, including: (i) the lost or diminished value of their Private Information; (ii) costs associated with the prevention, detection, and recovery from identity theft, tax fraud, and other unauthorized use of their data; (iii) lost opportunity costs to mitigate the Data Breach's consequences, including lost time; and (iv) emotional distress associated with the loss of control over their highly sensitive Private Information.

13. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their Private Information, but Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

14. Plaintiff, on behalf of herself and members of the proposed Class, therefore brings this lawsuit seeking damages and relief for Defendant's actions.

PARTIES

15. Plaintiff Jennifer Bandy is a current patient of TOC. She resides in Tennessee and intends to remain in Tennessee.

16. Defendant TOC Enterprises, Inc., d/b/a Tennessee Orthopaedic Clinics, is a division of Tennessee Orthopaedic Alliance, P.A. and has its principal place of business at 9129 Cross Park Dr., Ste. 101, Knoxville, Tennessee 37923. It can be served through its registered agent Michael T. Casey at that business address.

17. Tennessee Orthopaedic Alliance, P.A. has its principal place of business at 608 Norris Ave., Nashville, Tennessee 37204. It can be served through its registered agent Dr. William B. Kurtz, MD at 8 City Blvd., Suite 300, Nashville, Tennessee 37209.

18. Defendant TOC has other clinic or hospital locations in Tennessee, including, but not limited to locations in Knoxville, Louisville, Sevierville, Lenoir City, and Oak Ridge, Tennessee.

19. The names and capacities of persons, entities, associates, and/or corporations who may be responsible for some of the claims alleged in this Complaint are currently unknown to Plaintiff. If necessary, Plaintiff will seek leave of Court to amend this Complaint to reflect the true names and capacities of other responsible parties as their identities are learned.

JURISDICTION & VENUE

20. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the Class is a citizen of a state different from Defendant.

21. This Court has personal jurisdiction over Defendants because Defendant Tennessee

Orthopaedic Alliance, P.A. has its principal place of business within this District.

22. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Defendant Tennessee Orthopaedic Alliance, P.A. resides within this judicial district and a substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

BACKGROUND FACTS

TOC's Failure to Safeguard Patients' Private Information

23. TOC offers comprehensive medical and surgical treatment of bone, joint and soft tissue disorders[4], for which TOC requires that patients disclose their personal information in order to receive TOC's services.

24. Upon information and belief, the Private Information collected from current and former patients, as well as employees, includes their first and last names, dates of birth, addresses, email addresses, telephone numbers, patient identification numbers, insurance card numbers, their credit card information, Social Security numbers (for some), and medical information.

25. When TOC collects this sensitive information, it promises to use reasonable measures to safeguard Private Information from theft and misuse.

26. In fact, TOC informs its patients and their guardians that it collects and maintains their Private Information through the Privacy Policy (the "Privacy Policy").[5]

27. The Privacy Policy highlights TOC's legal obligations under federal and state law. It states, in part, that it "is being provided to you as a requirement of a federal law, the Health Insurance Portability and Accountability Act (HIPAA). This Privacy Notice describes how we

[4] https://www.tocdocs.com/ (last accessed July 20, 2023).
[5] https://www.tocdocs.com/privacy-policy/ (last accessed July 20, 2023).

may use and disclose your protected health information to carry out treatment, payment, or health care operations." TOC admits that it is "required by law to maintain the privacy of your health information and to provide you with this Privacy Notice of our legal duties and privacy practices with respect to protected health information. We are required by law to notify you if a breach of your unsecured protected health information occurs."[6]

28. TOC represented to its patients that their Private Information would be secure. Plaintiff and members of the proposed Class relied on such representations when they agreed to provide their Private Information to TOC.

29. Despite its alleged commitments to securing sensitive patient data, TOC does not follow industry standard practices in securing patients' Private Information.

30. In March 2022, hackers bypassed TOC's security safeguards and infiltrated its systems, giving them unfettered access to patients' Private Information.

31. Upon information and belief, the Data Breach was completely undetected for at least four days, during which time the hackers had unfettered access to the Private Information.

32. In response to the Data Breach, in its Breach Notice TOC contends that it has "implemented additional safeguards and technical security measures to further protect and monitor [its] systems." Ex. A. These measures should have been in place *before* the Data Breach.

33. TOC's website Breach Notice omits the size and scope of the breach. TOC has demonstrated a pattern of providing inadequate notice and disclosures about the Data Breach as it also notified HHS that the PHI of "500" individuals was affected, a placeholder number rather than actual number of individuals affected.

34. Upon information and belief, the Data Breach has impacted at least thousands

[6] *Id.*

former and current TOC patients.

35. Upon information and belief, TOC does not adequately train its employees on cybersecurity policies, enforce those policies, or maintain reasonable security practices and systems.

36. TOC's negligent conduct caused the Data Breach. TOC violated its obligation to implement best practices and comply with industry standards concerning computer system security. TOC failed to comply with security standards and allowed its patients' PII to be accessed and stolen by failing to implement security measures that could have prevented, mitigated, or timely detected the Data Breach.

37. To-date, TOC has not offered breach victims any identity theft protection services at all.

38. Plaintiff and the members of the proposed Class's personal data may exist on the dark web and in the public domain for months, or even years, before it is used for ill gains and actions.

39. Plaintiff and the members of the proposed Class have a real and cognizable interest in obtaining equitable relief, in addition to the monetary relief requested herein.

The Data Breach Was a
Foreseeable Risk of which TOC Was on Notice.

40. It is well known that PII, including Social Security numbers in particular, is a valuable commodity and a frequent, intentional target of cyber criminals. Companies that collect such information, including TOC, are well-aware of the risk of being targeted by cybercriminals.

41. Individuals place a high value not only on their PII, but also on the privacy of that data. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

42. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice, "[a] direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss."[7]

43. Individuals, like Plaintiff and Class members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and is likened to accessing your DNA for hacker's purposes.

44. Data Breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiff and Class members cannot obtain new numbers unless they become a victim of Social Security number misuse.

45. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So, using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and

[7] "Victims of Identity Theft, 2018," U.S. Department of Justice (April 2021, NCJ 256085) available at: https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed July 20, 2023).

address, remains the same."[8]

46. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[9]

47. Additionally in 2021, there was a 15.1% increase in cyberattacks and data breaches since 2020. Over the next two years, in a poll done on security executives, they have predicted an increase in attacks from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[10]

48. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, and hopefully can ward off a cyberattack.

49. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data."[11] This publication also explains that "[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."[12]

50. Despite the prevalence of public announcements of data breach and data security

---

[8] https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed July 20, 2023).
[9] https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last accessed July 20, 2023).
[10] https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 (last accessed July 20, 2023).
[11] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last accessed July 20, 2023).
[12] *Id.*

compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, TOC failed to take appropriate steps to protect the PII of Plaintiff and the proposed Class from being compromised.

TOC's Conduct Violates HIPAA.

51. HIPAA requires covered entities such as Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information (PHI).

52. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

53. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

54. A data breach such as the one Defendant experienced, is considered a breach under the HIPAA rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. § 164.40.

55. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate it failed to comply with safeguards mandated by HIPAA regulations.

Data Breaches Are Rampant in Healthcare.

56. TOC's data security obligations were particularly important given the substantial increase in data breaches in the healthcare industry preceding the date of the Breach.

57. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents."[13]

58. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[14]

59. The HIPAA Journal article goes on to explain that patient records, like those stolen from TOC, are "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[15]

60. Data breaches such as the one experienced by Defendant TOC have become so

[13] https://www.hipaajournal.com/why-do-criminals-target-medical-records/ (last accessed July 20, 2023).
[14] *Id.*
[15] *Id.*

notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, can prepare for, and hopefully can ward off a potential attack.

61. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[16]

62. According to Advent Health University, when an electronic health record "lands in the hands of nefarious persons the results can range from fraud to identity theft to extortion. In fact, these records provide such valuable information that hackers can sell a single stolen medical record for up to $1,000."[17]

63. The significant increase in attacks in the healthcare industry, and attendant risk of future attacks, is widely known to the public and to anyone in that industry, including Defendant TOC.

Plaintiff's Experience

Plaintiff Jennifer Bandy

64. Plaintiff Jennifer Bandy is a current TOC patient who received medical services from TOC. In exchange for those medical services, she provided her own Private Information (PII and PHI) to TOC, reasonably expecting that TOC would protect that Private Information as it promises to do through its Privacy Policy.

65. On approximately July 17, 2023, Plaintiff Bandy received a Notice Letter informing her that TOC identified that "some or all" of her Private Information was among the files breached during the "security incident." *See* Plaintiff Bandy's redated Notice Letter, attached in collective

[16] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last accessed July 20, 2023).
[17] https://www.ahu.edu/blog/data-security-in-healthcare (last accessed July 20, 2023).

Exhibit A.

66. Plaintiff Bandy is aware of the seriousness of protecting her Private Information and of data privacy since last year she was notified by the FBI that there were multiple loans taken out fraudulently in her name and that it had discovered her Private Information was being used fraudulently. She is concerned that the Private Information stolen from TOC can be put together in a "Fullz Package" to merge unregulated data available elsewhere to criminally stolen data as described below in Footnote 20.

67. Plaintiff Bandy reasonably believed that TOC utilized reasonable data security measures, such that her Private Information would be safe.

Plaintiff and Class Members

68. As a condition of receiving TOC's medical services, TOC required that both adult and minor patients (through their parents and/or legal guardians) provide their Private Information. Each of the Plaintiff and Class Members provided their Private Information to TOC.

69. Plaintiff reasonably believed that, as part of the payments to TOC for medical treatment and services, those payments included amounts for data security that would be included in general overhead costs of TOC. Had Plaintiff known that TOC did not utilize reasonable data security measures, they would have paid less for those treatments and services or sought treatment elsewhere.

70. Furthermore, Plaintiff's and her family's sensitive PII remains in TOC's possession without adequate protection against known threats, exposing them to the prospect of additional and future harm in the event TOC suffers another data breach.

71. Plaintiff is aware and concerned that her Private Information is at risk of being used for fraudulent purposes for many years as a result of the Data Breach.

Plaintiff and Class Members
Face Significant Risks of Continued Identity Theft

72. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

73. The ramifications of Defendant's failure to keep the Class members' Private Information secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

74. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[18]

75. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and

[18] *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims*, ThreatPost.com (Feb. 21, 2013), https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/ (last visited June 11, 2023).

fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in their possession.

76. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.[19]

77. The value of the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

78. Of particular importance here, a minor's Private Information can be stolen and used until the minor turns eighteen years old before the minor even realizes he or she has been victimized.

79. It can take both minor and adult victims years to spot identity or PII theft, giving criminals plenty of time to use that information for cash.

80. One such example of criminals using PII for profit is the development of "Fullz"

[19] *See Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited June 11, 2023).

packages.[20] Cybercriminals can cross-reference multiple sources of Private Information to merge unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

81. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link the new information to Plaintiff's and the Class members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cybercriminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact to find that members of the proposed Class's stolen PII is being misused, and that the misuse is fairly traceable to the Data Breach.

82. Defendant opened up, disclosed, and exposed the PII of members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open

[20] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY, (Sep. 18, 2014), *available at* https://krebsonsecurity.com/tag/fullz/ (last visited Jun 11, 2023).

unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

83. The risk to minor Class members is substantial given children's lack of established credit because their information can be used to create a "clean identity slate." It is not surprising, then, that one report found that children are 51% more likely be victims of identity theft than adults. Cybercriminals on the dark web have been caught selling Social Security numbers of infants for $300 per number to be used on fraudulent tax returns.[21]

84. Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed the Private Information of potentially thousands of members of the proposed Class to unscrupulous criminals.

85. Defendant's failure to properly notify members of the proposed Class of the Data Breach exacerbated their injuries by depriving them of the earliest ability to take appropriate measures to protect their family's PII and take other necessary steps to mitigate the harm caused by the Data Breach.

CLASS ACTION ALLEGATIONS

86. Plaintiff sues on behalf of herself and the proposed Class ("Class"), defined as follows:

> All individuals whose PII was compromised in the Data Breach discovered by Tennessee Orthopaedic Clinics in or about May 2023.

87. The following people are excluded from the Class: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries,

[21] Avery Wolfe, *How Data Breaches Affect Children*, Axion Cyber Sols. (Mar. 15, 2018), https://axiomcyber.com/data-breach/how-data-breaches-affect-children/ (last accessed June 10, 2023).

parents, successors, predecessors, affiliated entities, and any entity in which Defendant or its parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

88. Plaintiff reserves the right to amend the Class definition.

89. Numerosity, Fed. R. Civ. P. 23(a)(1): Class members are so numerous that joinder of all members is impracticable. Upon information and belief, there are thousands of individuals whose Private Information may have been improperly accessed in the Data Breach, and each Class member is apparently identifiable within Defendant's records.

90. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class members. These include:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class members ;

b. Whether Defendant had duties not to disclose the Private Information of Plaintiff and Class members to unauthorized third parties;

c. Whether Defendant had duties not to use the Private Information of Plaintiff and Class members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and

Class members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class members ;

k. Whether Defendant violated the consumer protection statutes invoked herein;

l. Whether Plaintiff and Class members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

m. Whether Plaintiff and Class members are entitled to restitution as a result of Defendant's wrongful conduct; and

n. Whether Plaintiff and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

91. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class members because all had their Private Information compromised as a result of the Data Breach, due to Defendant's misfeasance.

92. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class members, in that the Plaintiff's and Class members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy. Defendant's policies challenged herein apply to and affect Class members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

93. Adequacy of Representation, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and

adequately represent and protect the interests of the Class members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

94. Superiority, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

95. The nature of this action and the nature of laws available to Plaintiff and Class members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced

by the Class and will establish the right of each Class member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

96. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, including its privacy policy, uniform methods of data collection, the consistent provisions of the relevant laws, and the ascertainable identities of Class members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

97. Unless a class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class members, Defendant may continue to refuse to provide proper notification to Class members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

98. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

99. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiff and Class members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class members that their Private Information had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class members; and

i. Whether Class members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

100. Adequate notice can be given to Class members directly using information maintained in Defendant's records.

CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

101. Plaintiff and members of the Class incorporate all previous paragraphs as if fully set forth herein.

102. Plaintiff and members of the Class entrusted their and, for some, their minor children's PII to Defendant. Defendant owed to members of the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

103. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard the PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of the PII of Plaintiff and members of the Class by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

104. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of the PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Class to take appropriate measures to protect the PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

105. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and members of the Class's personal information and PII.

106. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

107. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing of the PII of Plaintiff and members of the Class, particularly because some of TOC's patients are minors, and the importance of exercising reasonable care in handling it.

108. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and members of the Class which actually and proximately caused the Data Breach and Plaintiff's and members of the Class's injury.

109. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

110. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of the PII by criminals, improper disclosure of the PII, lost benefit of the bargain, lost value of the PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence Per Se
(On Behalf of Plaintiff and the Class)

111. Plaintiff and members of the Class incorporate all previous paragraphs as if fully set forth herein.

112. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard the PII of Plaintiff and members of the Class.

113. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, patients' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect the PII of Plaintiff and members of the Class.

114. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect the PII of Plaintiff and members of the Class and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to its patients and former patients (and potentially employees) in the event of a breach, which ultimately came to pass.

115. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

116. Defendant had a duty to Plaintiff and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard the PII of Plaintiff and members of the Class.

117. Defendant breached its respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII of Plaintiff and members of the Class.

118. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

119. Further, Tennessee's Identity Theft Deterrence Act ("ITDA"), under T.C.A § 47-18-2107, required Defendant to notify all Tennessee residents whose "personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made no later than forty-five (45) days from the discovery or notification of the breach of system security[.]"

120. In other words, the ITDA imposed a statutory duty on Defendant to notify Plaintiff and the Class about the Data Breach within the statute's timeframe, which has not occurred to date.

121. Plaintiff and the Class belong to the class of persons the ITDA was designed to protect because they are Data Breach victims entitled to timely notice of the Data Breach.

122. Plaintiff's and the Class's injuries, including those caused by Defendant's untimely notice, are the types of injuries the ITDA was designed to protect against in requiring timely notice. Indeed, the ITDA's timing requirements are designed to give Data Breach victims an opportunity to mitigate the Data Breach's impact on them and safeguard their identities from theft.

123. Upon information and belief, Defendant's ongoing delay in notifying Plaintiff and the Class about the Data Breach was not "due to the legitimate needs of law enforcement" as

defined by ITDA.

124. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

125. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

126. Had Plaintiff and members of the Class known that Defendant did not adequately protect their PII, Plaintiff and members of the Class would not have entrusted Defendant with their Private Information.

127. As a direct and proximate result of Defendant's negligence per se, Plaintiff and members of the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

COUNT III
Breach of an Implied Contract
(On Behalf of Plaintiff and the Class)

128. Plaintiff and members of the Class incorporate all previous paragraphs as if fully set forth herein.

129. Defendant offered to provide medical services to Plaintiff (including minor children) and members of the Class in exchange for their PII and in exchange for amounts paid for

medical treatment and services that included payment for data security.

130. In turn, and through internal policies, Defendant agreed it would not disclose the PII it collects to unauthorized persons. Defendant also promised to safeguard patient PII.

131. Plaintiff and the members of the Class accepted Defendant's offer by providing PII to Defendant in exchange for medical services.

132. Implicit in the parties' agreement was that Defendant would provide Plaintiff and members of the Class with prompt and adequate notice of all unauthorized access and/or theft of their PII.

133. Plaintiff and the members of the Class would not have entrusted their and their children's PII to Defendant in the absence of such agreement with Defendant.

134. Defendant materially breached the contract(s) it had entered with Plaintiff and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant further breached the implied contracts with Plaintiff and members of the Class by:

a. Failing to properly safeguard and protect the PII of Plaintiff and members of the Class;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PII that Defendant created, received, maintained, and transmitted.

135. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

136. Plaintiff and members of the Class have performed as required under the relevant

agreements, or such performance was waived by the conduct of Defendant.

137. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

138. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

139. Defendant failed to advise Plaintiff and members of the Class of the Data Breach promptly and sufficiently.

140. In these and other ways, Defendant violated its duty of good faith and fair dealing.

141. Plaintiff and members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

142. Plaintiff and members of the Class incorporate all previous paragraphs as if fully set forth herein.

143. This claim is pleaded in the alternative to the breach of implied contract claim.

144. Plaintiff and members of the Class conferred a benefit upon Defendant in the form

of monies paid for treatment services and by providing their PII to Defendant in order to receive such services.

145. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and members of the Class.

146. As a result of Defendant's conduct, Plaintiff and members of the Class suffered actual damages in an amount equal to the difference in value between the purchases made with reasonable data privacy and security practices and procedures that Plaintiff and members of the Class paid for, and the purchases without unreasonable data privacy and security practices and procedures that they received.

147. Under the principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the proposed Class's payments and their PII because Defendant failed to adequately protect their PII. Plaintiff and the proposed Class would not have provided their PII, nor used and paid for Defendant's services, had they known Defendant would not adequately protect their PII.

148. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by it because of its misconduct and the Data Breach alleged herein.

COUNT V
Violation of the Tennessee Consumer Protection Act,
Tenn. Code Ann. §§ 47-18-101, *et seq*.
(On Behalf of Plaintiff and the Class)

149. Plaintiff and members of the Class incorporate all previous paragraphs as if fully set forth herein.

150. Tennessee's Identity Theft Deterrence Act ("ITDA"), under T.C.A § 47-18-2106, states that any violation of the ITDA "constitutes a violation of the Tennessee Consumer Protection

Act[,]" ("CPA"). The ITDA further states: "For the purpose of application of the [CPA], any violation of this part shall be construed to constitute an unfair or deceptive act or practice affecting trade or commerce and subject to the penalties and remedies as provided in that act, in addition to the penalties and remedies set forth in this part."

151. Defendant violated the ITDA because Defendant did not follow its provisions in notifying Plaintiff and the Class about the Data Breach.

152. During the Data Breach, Defendant suffered a "breach of system security" as the ITDA defines that term. Upon information and belief, Defendant maintained the PII of Plaintiff and members of the Class in an unencrypted form, as defined in Tenn. Code Ann. § 47-18-2107(a).

153. The ITDA defines "information holder" to include Defendant because Defendant conducts business in Tennessee.

154. In Tenn. Code Ann. § 47-18-2107(a)(4), the ITDA defines "personal information" to include Plaintiff's and the Class's PII, including their names in combination with the Social Security numbers, driver's license numbers, or any "Account, credit card, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account[.]"

155. Following discovery of the Data Breach caused by unauthorized actors, the ITDA required Defendant to notify all Tennessee residents whose "personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made no later than forty-five (45) days from the discovery or notification of the breach of system security[.]" On information and belief, Defendant's ongoing delay in notifying Plaintiff and the Class about the Data Breach was not "due to the legitimate needs of law enforcement" as defined by ITDA.

156. Defendant failed to disclose the Data Breach to Plaintiff and the Class within 45 days of discovering it, meaning it violated the CPA.

157. As a direct and proximate cause of Defendant's ITDA and CPA violations, Plaintiff and the Class have suffered damages, including (i) the compromise, publication, and/or theft of the PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (iii) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (iv) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession, and (v) future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

158. Plaintiff and the Class are entitled to damages as well as injunctive relief, including, but not limited to, ordering Defendant to: (i) strengthen its data security systems, monitoring procedures, and data breach notification procedures; and (ii) immediately provide adequate credit monitoring to Plaintiff and the Class.

COUNT VI
Violation of the ITDA under Tenn. Code Ann. § 47-18-2104
(On behalf of Plaintiff and the Class)

159. Plaintiff and members of the Class incorporate all previous paragraphs as if fully set forth herein.

160. As explained in this Complaint, Defendant violated the ITDA in failing to give notice of the Data Breach according to its provisions, including failure to notify all Tennessee

residents whose "personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made no later than forty-five (45) days from the discovery or notification of the breach of system security[.]"

161. Under Tenn. Code Ann. § 47-18-2104(f), "[w]ithout regard to any other remedy or relief to which a person is entitled, anyone affected by a violation of this part may bring an action to obtain a declaratory judgment that the act or practice violates this part and to enjoin the person who has violated, is violating, or who is otherwise likely to violate this part[.]"

162. Defendant has, is, and is likely to violate the ITDA because Defendant failed to give Plaintiff and the Class notice of the Data Breach according to the ITDA's terms, its Breach Notice is and was inadequate, and Defendant has not developed or maintained adequate policies and procedures to comply with the ITDA's terms.

163. Further, under § 47-18-2104(f), "Upon a finding by the court that a provision of this part has been violated, the court may award to the person bringing such action reasonable attorneys' fees and costs."

164. Plaintiff and the Class are thus entitled to a declaratory judgment that Defendant violated the ITDA and are entitled to an injunction ordering Defendant to: (i) strengthen its data security systems, monitoring procedures, and data breach notification procedures; and (ii) immediately provide adequate credit monitoring to Plaintiff and the Class.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Dated: October 25, 2023

Respectfully submitted,

MASON LLP

/s/ Lisa A. White

Lisa A. White (TN BPR # 026658)
lwhite@masonllp.com
Gary E. Mason*
gmason@masonllp.com
Danielle L. Perry*
dperry@masonllp.com
MASON LLP (primary office address)
5335 Wisconsin Ave. NW, Ste. 640
Washington, DC 20015
Phone: (202) 429-2290

**Pro Hac Vice*

Attorneys for Plaintiff and the Proposed Class